ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

Distributed Clone Attack detection Protocols in Static Wireless Sensor Networks: A survey

J.Anthoniraj[1], Dr.T.Abdul Razak[2]

Research Scholar, Bharathidasan University, Trichy, India[1]

Associate Professor, Jamal Mohamed College, Trichy, India[2]

Abstract: Wireless Sensor Network (WSN) consists of sensor nodes which senses, computes and has wireless communication capabilities. WSN is deployed in unattended and unsecure environments. An adversary can easily capture one node from the network and create a clone of a captured node. Then, these clones can be deployed in all network areas, and they can be considered as legitimate members of the network. So it is difficult to detect a replicated node. In distributed environment many protocols are available to detect the clone attack. In this paper, we review these protocols and compare their performance with the help of witness selection, communication and memory overhead, detection probability of replicated nodes and resilience against node compromise.

Keywords: Wireless Sensor Networks, Base station, Clone attack Witness node, Cluster based.

I. INTRODUCTION

WSN is a collection of spatially distributed autonomous sensors to monitor physical [or] environmental conditions[1]. It has tiny sensor nodes, consisting of sensing, data processing and communication components[2]. It is composed of a large number of sensor nodes that are densely deployed in harsh environments to fulfill both military and civil applications[3]. It consists of a base station that can communicate with a number of wireless sensors via a radio link. Data is collected at the wireless sensor node, compressed and transmitted to the base station directly[4]. It suffers from many constraints including low computation capability, small memory, limited energy resources, use of insecure wireless communication channels and deployment of sensor node in an unattended environment these constraints make security in WSN a challenge[2,5]. Different possible attacks on WSN are selective forwarding attack, sinkhole attack, wormholes attack, sybil attack, HELLO flood attack, acknowledgement spoofing, sniffing attack, data integrity attack, energy drain attack, black hole attack, denial of service attack, physical attacks, traffic analysis attack, privacy violation by attack and clone attack[6,7,8].
The rest of this paper is organized as follows. Section 2 describes about clone attack. In section 3, we have discussed about the clone attack detection. In section 4, the different distributed approaches to detect clone attacks are briefly reviewed. In section 5, we present a comparison between these protocols . The main drawbacks of these protocols are listed in section 6. Finally section 7 presents the concluding remarks.

II. CLONE ATTACK

An adversary can capture a sensor node and extract its key materials. Once a node is captured, the attacker can reprogram it and create a clone of a captured node. These clones (or) replicas can be deployed in all network areas. These replica node attacks are very dangerous to the operations of sensor networks. With a single captured sensor node, the adversary can create as many replica nodes as he wants. The replica nodes are controlled by the adversary, but have key materials that allow them to seem like authorized participants in the network. So it is very much difficult to detect a clone attack[9].

III. CLONE ATTACK DETECTION

WSN can be either static or mobile. In static WSN sensor nodes are deployed randomly and after deployment their positions do not change. In mobile WSN, the sensor nodes can move their own after deployment. Many approaches have been proposed to detect clone attack in static WSNs which are broadly categorized into centralized and distributed techniques. In a centralized approach for detecting node replication, when a new node joins the network, it broadcasts a signed message (location claim) containing its location and identity to its neighbors. One or more of its neighbors then forward this location claim to a central trusted party (base station). With location information for all the nodes in the network, the central party can easily detect any pair of nodes with the same identity but at different locations. Distributed approaches for detecting node replications are based on location information for a node being stored at one or more witness nodes in the network. When a new node joins the network, its location claim is forwarded to the corresponding witness nodes. If any witness node receives two different location claims for the same node Identity (ID), then the existence of replica is detected[10]. Some of the protocols using distributed approaches for static WSN are introduced in the following paragraphs.

IV. DISTRIBUTED CLONE ATTACK DETECTION PROTOCOLS FOR STATIC WSN

1) Broadcast Protocol

Each node in the network uses an authenticated broadcast message to flood the network with its location information. Each node stores the location information for its neighbors. If it receives a conflicting claim, it revokes the offending node[11].

2) Deterministic Multicast (DM) Protocol
Each node shares a node's location claim with a limited subset of deterministically chosen by witness nodes. When a node broadcasts its location claim, its neighbors forward that claim to a subset of nodes called witnesses. The witnesses are chosen as a function of the node's ID. If the adversary replicates a node, the witnesses will receive two different location claims for the same node ID. The conflicting location claims become an evidence to trigger the revocation of the replicated node[11].

3) Randomized Efficient and Distributed (RED) Protocol
The base station broadcasts a random value to all nodes in the network. Each node broadcasts a location claim to its neighbors. Then each neighbor selects a witness node to forward the location claim. The witness node selection based on a pseudo random function with the inputs of node`s ID, the random value which is broadcasted by the base station and the number of destination locations. Location claims with the same node ID will be forwarded to same witness nodes in each detection phase. Hence, the replicated nodes will be detected in each detection phase. Next time when the protocol executes, the witness nodes will be different since the random value which is broadcasted by the base station is changed[12].

4) Randomized Multicast (RM) Protocol
In this protocol, each node broadcasts its location claim, along with a signature authenticating the claim. Each of the node`s neighbors probabilistically forward the claim to a randomly selected set of witness nodes. If any witness receives two different location claims for the same node ID it can revoke the replicated node[11].

5) Line Selected Multicast (LSM) Protocol
In this protocol, when a node announces its location, every neighbor first locally checks the signature of the claim and then forwards it to randomly selected destination nodes. A location claim, when travelling from source to destination, it has to pass through several intermediate nodes that form claim message path. Node replication is detected by the node on the intersection of two paths generated by two different node claims carrying the same ID and coming from two different nodes[13].

6)Localized Multicast Protocols
6.1) Single Deterministic Cell (SDC)
In this protocol, the node broadcasts its location claim, each neighbor, first verifies the validity of the signature in the location claim. Each neighbor independently decides whether to forward the claim. If a neighbor plans to forward the location claim, it first needs to execute a geographic hash function to determine the destination cell. Once the location claim arrives at the destination cell, the sensor receiving the claim first verifies the validity of the signature. The location claim is flooded within the destination cell. Whenever any witness receives a location claim with the same identity but a different location compared to a previously stored claim, it forwards both location claims to the base station. Then, the base station will broadcast a message within the network to revoke the replicas[14].

6.2) Parallel Multiple Probabilistic Cells (P-MPC)
In P-MPC the location claim is mapped and forwarded to multiple deterministic cells with various probabilities. When a node broadcasts its location claim, each neighbor independently decides whether to forward the claim in the same way as in the SDC scheme. The neighbors that forward the claim can determine the destination cell based on a geographic hash cells to which the identity of the sender are mapped, based on a geographic hash function[10]

7)Memory Efficient Multicast Protocols
7.1) Memory Efficient Multicast using Bloom filters(B-MEM)
This protocol forwards a location claim to a randomly selected locations on a line segment. All the intermediate nodes on the line serve as watchers while the first and last node serve as witnesses. When a node receives the location claim, it performs the two-phase conflict check to detect conflict claims[15].

7.2) Memory Efficient Multicast using Bloom filters and Cell forwarding (BC-MEM)
In this protocol, the deployment area is divided into virtual cells. In each cell, an anchor point is assigned for every node in the network. The node close to the anchor point is called anchor node. The location claim is forwarded to the anchor point of the next cell where the line segment interacts. The claim is then forwarded from one anchor node to another until it reach at the last cell. The anchor nodes in the intermediate cells are watchers and the anchor nodes in the first and last cells are witnesses[15].

8)Hierarchical Distributed Algorithm(HDA)
This protocol has three steps. In the first step, all the material required for Bloom filter computations and for cryptographic operations follow the tree hierarchical architecture. The sensor nodes send their data only to their cluster heads. The cluster heads forward them to the base station. Cluster heads communicate with each other through dedicated paths and create a kind of tree with base station as a root. The detection is performed by the cluster nodes using a Bloom filter mechanism and based on the hierarchical architecture of the wireless sensor networks[16].

9)Random Walk Based Protocols
9.1) RAndom WaLk (RAWL)
Each node broadcasts a signed location claim. Each of the node's neighbors probabilistically forwards the claim to some randomly selected nodes. Each randomly selected node sends a message containing the claim to start a random walk in the network. The passed nodes are selected as witness nodes, and it will store the claim. If any witness node receives different location claims for a same node ID, then a replicated node is detected[17].

9.2) Table-asssisted RAndom WaLk (TRAWL)
In this protocol, when a randomly chosen node starts a random walk, all the passed nodes will become witness nodes. However, they do not definitely store the location

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

claim, instead, they store the location claim independently. Also, each witness node will create a new entry in its trace table for recording the pass of a location claim. When receiving a location claim, a node will first find the entries which have the same node ID as the claim in its trace table. If any entry is found, the node will compute the digest of the claim and compare the digest with the digest in the entry. When two digests are different, the node detects a clone attack[17].

10)Detection of Node Capture Attack(DNCA)

In this protocol, the physically captured nodes are not present in the network during the period from the captured time to the redeployment time. The captured nodes do not participate in any network operation during this period. The captured node can be identified by sequential probability ratio test. The protocol then measures the absence time period of a sensor node and compares it to a predefined threshold. If it is more than threshold value, the sensor node is considered as a captured node[18].

11)Cell based Identification of NOde Replication Attack (CINORA)

In this method, a sensor network is divided into geographical cells similar to the existing cellular network. In this protocol, location claim from the nodes are distributed among a subset of cells to detect any replication. These cells are generated from a non null intersecting subset algorithm. During the authentication phase, at least one cell receives conflicting location claims, if adversary has ever attempted to replicate a legitimate node[19].

V. COMPARISON OF PROTOCOLS

The performance of the distributed clone attack detection protocols can be evaluated with help of witness selection, memory and communication overhead, detection probability of replicated nodes and resilience against node compromise. Table I represents various type of schemes used to detect clone attacks in the distributed protocols.

TABLE I
TYPE OF SCHEMES IN THE PROTOCOLS

No	Protocol	Type of Scheme used
1	broadcast	Network broadcast
2	DM	Witness based
3	RED	Witness based
4	RM	Witness based
5	LSM	Witness based
6	SDC	Witness based
7	P-MPC	Witness based
8	B-MEM	Witness based
9	BC-MEM	Witness based
10	HDA	Cluster based
11	RAWL	Witness based
12	TRAWL	Witness based
13	DNCA	Base station based
14	CINORA	Group based

A) Witness node Selection

RM protocol distributes location claims to randomly selected set of witness nodes[11]. In LSM protocol a location claim, when travelling from source to destination has to pass through several intermediate nodes. The Table I represents various type of schemes used in the distributed protocols. LSM was developed as a less expensive version of RM, but it suffers from uneven distribution of witness nodes[13]. RED is similar in principle, to the RM protocol but with witness chosen pseudo randomly based on a network-wide seed[13].In SDC and P-MPC protocols the witness nodes for a node identity are randomly selected from the nodes that are located within a geographically limited region[14]. In P-MPC the location claim is forwarded to multiple deterministic cells with various probabilities by executing a geographic hash function[20]. B-MEM stores the information about a location claim and allows them to the randomly selected line segments, which are likely to pass the center area of the deployment. BC-MEM requires highly accurate localization due its cell division and anchor node selection[15].The BC- MEM protocol does not forward a claim on the line segment. It forwards the claim to the anchor point in the next cell that the line segment intersects. RAWL protocol starts several random walks randomly in the network for each node *x* ,and then selects the passed nodes as the witness nodes of node *x*[17].

B) Communication Overhead

Table II represents communication costs used in various distributed clone attack detection protocols. Table III represents various notations used in Table II and Table IV.

TABLE II
COMMUNICATION COST

No	Protocol	Communication cost
1	broadcast	$O(n^2)$
2	DM	$O(glog\sqrt{n}/d)$
3	RED	$O(r.\sqrt{n})$
	RM	$O(n^2)$
5	LSM	$O(n\sqrt{n})$
6	SDC	$O(r.\sqrt{n})$-$O(s)$
7	P-MPC	$O(r.\sqrt{n})$-$O(s)$
8	B-MEM	$O(kn\sqrt{n})$
9	HDA	$O(N^2)$
10	RAWL	$O(\sqrt{n}logn)$
11	DNCA	$O(n\sqrt{n})$

TABLE III
NOTATIONS

n	Number of nodes in the network
g	Number of witnesses selected by each neighbor
d	Average degree of each node
s	Number of nodes in a cell
l	The node sending the location claim
w	The number of the witness nodes that store the local claim
r	Communication Radius.
N	Number of cluster heads
k	Average number of line segments for each claim
t	Size of a location claim
t^1	The number of bytes that a Bloom filter uses to record the membership of an element.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

The Broadcast protocol offers the simplest solution, but the communication overhead will only be tolerable for small network. DM improves on the communication requirements, by selecting a fixed set of witnesses. RM imposes communication overhead equal to that of the broadcast scheme[11].LSM scheme reduces the communication overhead of the RM scheme by having every claim-relaying node participate in the replica detection and revocation process. RED still has the same communication overhead as the LSM scheme[18]. RED produces a large improvement over RM in terms of communication[13].

The communication overheads of SDC and P-MPC will be slightly higher than that of RED in particular, when the network size is large. SDC has the lowest communication overhead though the differences between SDC, P-MPC and LSM are relatively small. As the network size increases P-MPC and SDC have lower overhead than LSM[14]. The communication overheads of RAWL and TRAWL protocols are higher than LSM[17].

C) Memory overhead

For networks in which the number of nodes is less than the square of the average degree, RM will tend to be more space efficient[11]. LSM requires to store a higher number of messages compared to RED, because in LSM, every node in a claim path is a possible witness, and therefore, has to store every claim it relays. In RED, only destinations can be witnesses, and thus, only destination are required to store the claims[13]. The memory overhead of the SDC is much lower than those of the RM and LSM protocols[10].Table IV represents memory costs used in various distributed clone attack detection protocols.

TABLE IV
MEMORY COST

No	Protocol	Memory cost
1	Broadcast	O(d)
2	DM	O(g)
3	RED	O(r)
4	RM	$O(\sqrt{n})$
5	LSM	$O(\sqrt{n})$
6	SDC	W
7	P-MPC	W
8	B-MEM	$O(tk+tk\sqrt{n})$
9	HDA	O(N)
10	RAWL	$O(\sqrt{n}\log n)$
11	TRAWL	$O(1)^2$
12	DNCA	O(n)

In LSM, a node stores a complete copy of each location claim it receives, some nodes may have to store several hundred location claims, which will exhaust their memory space. In B-MEM and BC-MEM protocols, a node exploits bloom filters to record the foot print of most location claims it receives and it only stores a few complete claims[15]. TRAWL is used to reduce the memory overhead of RAWL by using a table to cache the digests of location claims[17].

D) Detection of Replicated Nodes

The LSM protocol is similar to RM, but it introduces a remarkable improvement in terms of detection probability. RED has better detection probability and coverage faster than LSM for all practical values of the network parameters[13]. Compared to the RM and LSM algorithms, a major advantage of SDC is that it ensures more success rate for detecting any node replication[10]. B-MEM has a slight lower detection probability than LSM in some cases due to false positive of Bloom filters. BC-MEM achieves a higher detection probability than both LSM and B-MEM by using the cell forwarding technique[15]. HDA have more efficient detection probability than RM and LSM [16]. Both RAWL and TRAWL protocols have much higher detection probability than LSM[17].

E) Resilience against Node compromise

DM selects a fixed set of witnesses, adversary easily compromise witness nodes so it loses its resiliency. RM provides excellent resiliency, since it prevents the adversary from anticipating the identity of the witnesses. Finally, LSM provides comparable (or) greater resiliency[11]. RED is more resilient in its detection capabilities than LSM[13]. In SDC, witness nodes are chosen randomly from the nodes of a given cell instead of the whole network as in the RM protocol . Therefore assuming that the adversary`s capability of compromising nodes is limited. So that in SDC, the probability that an adversary can compromise all the witness nodes storing the location claim of a given identity is higher than of the RM protocol. Compared to SDC, P-MPC is more robust to node compromise[10].

VI. DRAWBACKS OF THE PROTOCOLS

The broadcast protocol has high communication and memory overhead for large sensor networks. The DM protocol does not provide much security, adversary easily compromises witness nodes[11]. Both RM and LSM are unable to detect masked replication attacks and sometimes location claims of clone nodes also received to the witness node[13]. The SDC protocol flooding only through the first copy of a node location claim arrives at the cell and the other copies are ignored. The node in the cell that first receives the location claim is unable to distinguish between claims of original and cloned node[14]. In RED protocol the deterministic selection of witness nodes and its infrastructure for distributing random seed may not always be available. It is unable to detect masked replication attacks[12]. Both RAWL and TRAWL protocols require more than twice the communication overhead of LSM[17].

VII. CONCLUSION

Wireless sensor networks are deployed in hostile environment and vulnerable to various types of attacks. This paper outlined the different types of attacks on WSN and mainly about clone attack. We have provide various approaches to find the cloned node. In this paper we have compared various static distributed protocols in that, we find that SDC protocol has lower communication cost than other protocols for smaller size network. The RED

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

protocol has the lowest communication overhead for larger network. The SDC protocol has lower memory overhead than other distributed protocols. The RED and BC-MEM protocols have better detection probability than other protocols. The P-MPC protocol has more resilience against node compromise than other protocols.

REFERENCES

[1] Wireless Sensor Network – Wikipedia, the free encyclopedia(“http:// en.wikipedia.org/ wiki/ wireless – sensor network’’).

[2] Yong Wang, Garhan Attebury and Byrav Ramamurthy “A survey of security networks issues in wireless sensor networks ‘IEEE Communications Surveys and Tutorials, vol. 8, no. 2, 2006.

[3] Ian F.Akyildiz, Weilian Su, Yogesh S.Subramaniam, and Erdal Cayirci, “A survey on sensor network”, IEEE Communications Magazine, pp 102-114, August 2002.

[4] Cris Townsend, Stevan Arms, “Wireless sensor network: principles and applications”, Chapter 22,pp 439 – 449.

[5] Dr.G.Padmavathi, Mrs. D.Shanmuga Priya, “A survey of attacks, security mechanisms and challenges in wireless sensor networks”, International Journal of Computer science and Information Security, Vol.4 ,no.1 & 2, 2009.

[6] Prabhudutta Mohanty, Sangram Panigrahi, Nityananda Sarma and Siddhartha Sankar Satapathy, “Security issues in wireless sensor network data gathering protocols: A Survey”, Journal of Theoretical and Applied Information Technology, pp 14-29, 2005-2010.

[7] Mona Sharifnejad, Mohsen sharifi, Mansoureh Ghiasabadi and sureh Beheshti. “A survey on wireless sensor networks security”, Fourth International Conference: Sciences of Electronic Technologies of Information and Telecommunication, March 25-29, 2007.

[8] Yan-XiaoLi, Lian-Qin, Qian-Liang, ‘‘Research on wireless sensor network security”, IEEE Computer Society, International Conference on Computational Intelligence and security, 2010.

[9] Jun-WonHo,Donggang Lin ,Matthew Wright, Sajai K.Das,” Distributed detection of replicas with deployment knowledge in wireless sensor networks”, Preprint submitted to Elsevier,March ,2009.

[10] Bio Zhu, Venkata Gopala Krishna Addada, Sanjeev Setia , Sushil Jajodia and Sankaradas Roy,“Efficient distributed detection of node replication attacks in sensor networks”,in Proceedings of the 23rd Annual Computer Security Applications Conference(ACSAC`07),pp 257 – 266,Miami Beach,Fla,USA,December 2007

[11] Bryan Parno, Adrian Perrig, Virgil Gligor, ” Distributed detection of node replication attacks in sensor networks “,in Proceeding of the IEEE Symposium on Security and Privacy,(IEEE S and P`05),pp49-63,May 2005.

[12] Mauro Conti, Roberto Di Pieto, L.V.Mancini and A.Mei,”A randomized and distributed protocol for the detection of node replication attacks in wireless sensor networks “, in the Proceedings of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing(MobiHoc`07),pp 80-89, September 2007.

[13] Mauro Conti, Roberto Di Pietro, Luigi Vincenzo Mancini and Alessandro Mei “Distributed detection of clone attacks in wireless sensor networks” IEEE Transactions on Dependable and Secure Computing, Vol 18,No. 5,pp685-698, 2011.

[14] Bio Zhu, Sanjeev Setia, Sushil Jajodia, Sankardas Roy and Lingyu Wang “Localized multicast: efficient and distributed replica detection in large-scale sensor networks”, IEEE Transactions on Mobile Computing, Vo1. 9, No. 7, pp 913-926, 2010.

[15] Ming Zhang, Vishal Khanapure, Shigang Chen,Xuelian Xiao, “Memory efficient protocols for detecting node replication attacks in wireless sensor networks”, in Proceedings of the 17th IEEE International Conference on Network Protocols (ICNP’09), pp 284-293, Princeton,NJ,USA,October,2009.

[16] Wassim Znaidi, Marine Minjer, Stephane Uheda,”Hierachical node replication attacks detection in wireless sensors networks “,in Proceedings of the 20th IEEE Personal, Indoor and Mobile Radio Communication Symposium(PIMRC’09), pp 82-86,Tokyo,Japan,September 2009.

[17] Yingpei Zeng, Jiannong Cao, Shigeng Zhang,Shanqing Gao and Li Xie “Random walk based approach to detect clone attacks in wireless sensor networks “, IEEE Journal on selected areas in Communications, Vol. 28, No.5, pp 677-691, 2010.

[18] J.W.Ho,”Distributed detection of node capture attack in wireless sensor networks”, in Smart Wireless Sensor Networks, pp 345-360,In Tech Europe,Rijeka,Groatia, 2010.

[19] S, Gautam Thakur “CINORA: Cell based Identification of Node Replication attacks in wireless sensor networks”, in proceedings of the IEEE International Conference on Communications Systems (ICCS -080, 2008).

[20] Lee-Chun Ko, Hung-Yuan Chen, Guan-Rong Lin,”A neighbor-based detection scheme for wireless sensor networks against node replication attacks”,in the proceedings of the International Conference on Ultra Modern Telecommunications and workshops(ICUMT`09), pp. 1-6, St.Petersburg,Russia,October 2009.